UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF WISCONSIN

UNITED STATES OF AMERICA,

Plaintiff,

v. Case No. 17-CR-124

MARCUS HUTCHINS,

Defendant.

UNITED STATES' RESPONSE TO DEFENDANT'S MOTION TO DISMISS THE INDICTMENT FOR FAILURE TO STATE AN OFFENSE AND MULTIPLICITY (DOC. #95)

The United States of America, by its attorneys, Matthew D. Krueger, United States Attorney for the Eastern District of Wisconsin, and Assistant U.S. Attorneys Michael Chmelar and Benjamin Proctor, files this response to defendant Marcus Hutchins's motion to dismiss the indictment. Doc. #95. In his motion to dismiss, Hutchins argues (a) that Counts One and Seven should be dismissed "because the indictment fails to allege any facts that [Hutchins] had any intent to cause 'damage' to a protected computer;" (b) Counts One through Six "fail to state an offense because Kronos and UPAS Kit are not an 'electronic, mechanical, or other device' as defined by the Wiretap Act; (c) Counts Two and Three are multiplicitous; and (d) Counts One, Four through Eight, and Ten fail to allege the necessary "intent and causation." Doc. #95 at 1-2. The government will discuss each complaint in turn.

As discussed below, each of the defendant's arguments are meritless and his motion should be denied.

A. Standard of Review.

Federal Rule of Criminal Procedure 12(b)(3)(B) allows a defendant to make a pretrial motion that challenges the sufficiency of the indictment. A defendant may challenge the indictment's sufficiency by arguing that it fails to state an offense. Fed. R. Crim. P. 12(b)(3)(B)(v). Federal Rule of Criminal Procedure 7(c)(1) requires an indictment to "be a plain, concise, and definite written statement of the essential facts constituting the offense charged."

The Seventh Circuit has explained that an indictment is sufficient where it (1) states the elements of the crimes charged, (2) adequately informs the defendant of the nature of the charges brought against him, and (3) enables the defendant to assert the judgment as a bar to future prosecutions for the same offense. *See United States v. Vaughn*, 722 F.3d 918, 925 (7th Cir. 2013). The Seventh Circuit has further explained that an indictment "that 'tracks' the words of a statute to state the elements of the crime is generally acceptable, and while there must be enough factual particulars so the defendant is aware of the specific conduct at issue, the presence or absence of any particular fact is not dispositive." *Id.* (quoting *United States v. White*, 610 F.3d 956, 958-59 (7th Cir. 2010)); *see also United States v. Resendiz-Ponce*, 549 U.S. 102, 109 (2007) (explaining that an indictment "parroting the language of a federal criminal statute" is sufficient so long as the crime is not one that must be charged with greater specificity).

B. Counts One and Seven state an offense.

Hutchins argues that Counts One and Seven, which allege violations of 18 U.S.C. §§ 371 and 1030, should be dismissed because those counts "fail to allege any facts that would show Mr. Hutchins had any intent to cause 'damage' to a protected computer . . . ." Doc. #95 at 1. The crux of his position is that the indictment is faulty because does not expressly state that Kronos and UPAS Kit (identified in the indictment as "malware" and a "banking Trojan") actually "damage" computers under 18 U.S.C. § 1030. Specifically, relying on paragraphs 1(e) and 1(f) of the superseding indictment, Hutchins argues that the indictment states "only that "Kronos 'recorded and exfiltrated user credentials and personal identifying information from protected computers," and UPAS Kit "allowed for the unauthorized exfiltration of information," which, according to Hutchins, simply means "making a copy of data and taking it away." Doc. #96 at 4-5. According to Hutchins, "making a copy of data and taking it away" is not a crime under federal law.

Hutchins is wrong for several reasons. First, Hutchins is misguided with regard to pleading requirements in federal criminal cases. Counts One and Seven "track" the language of sections 371 and 1030. Doc. #86. Count One alleges Hutchins knowingly conspired (entered an unlawful agreement) to violate section 1030 in violation of section 371, and Count Seven alleges Hutchins knowingly attempted and aided and abetted an attempt to cause damage to a protected computer. Doc. #86. Each count (1) states the elements of the crimes

charged, (2) adequately informs the defendant of the nature of the charges brought against him, and (3) enables the defendant to assert the judgment as a bar to future prosecutions for the same offense. *See Vaughn*, 722 F.3d at 925; Doc # 86. Each count complies with Federal Rule of Criminal Procedure 7(c)(1).

Hutchins wants, without overtly asking for it, this Court to employ civil pleading standards to a criminal case. But the Seventh Circuit has consistently held that civil pleading standards do not apply in criminal cases. For instance, in *Vaughn*, 722 F.3d at 926, the court rejected the defendant's request to adopt civil pleading standards to assess the sufficiency of a criminal indictment. *Id.* Instead, the court noted that if a defendant has "serious apprehension about his ability to prepare a defense in the light of the charges against him, he can file a bill of particulars." *Id.*; see also *United States v. Gerebizza*, No. 16-1725, 2017 WL 6540505, *3 (7th Cir. 2017)) (rejecting the defendant's complaint that the superseding indictment was defective because it contained "legal conclusions" and "naked assertions" that violate pleading standards in civil cases).

Second, Hutchins misunderstands the nature of the charges in Count One and Seven and the government's burden at trial. Conspiracy punishes an illegal agreement. *United States v. Read*, 658 F.2d 1225, 1240 (7th Cir. 1981) (describing liability for a conspiracy and mail fraud). And it is well established that under conspiracy law, the object of the conspiracy does not need to be achieved for liability to attach. *United States v. Donner*, 497 F.2d 184, 190 (7th Cir. 1974). Therefore,

the government only needs to prove Hutchins conspired to damage computers, not the actual damage he intended.

The same is true for Count Seven. An attempt is a substantial step towards completing the crime with the intent to complete the crime. *United States v. Sanchez*, 615 F.3d 836, 843-44 (7th Cir. 2010). As with Count One, the government does not have a burden to prove damage; only an attempt to damage.

Finally, and more importantly, Hutchins chooses to ignore the fact that the indictment states Kronos and UPAS Kit are forms of "malware," which by common knowledge are "[p]rograms written with the intent of being disruptive or damaging to (the user of) a computer or other electronic device; viruses, worms, spyware, etc., collectively." Oxford English Dictionary 2018, *available at* http://www.oed.com/view/Entry/ 267413?redirectedFrom=malware#eid (last visited April 18, 2018). And the superseding indictment (¶1(d)) defines "malware" as "malicious computer code intended to damage a computer . . . [that] deletes, creates, and modifies files on a computer . . . ." Doc. #86 at 2. So the superseding indictment alleges, although not required, an intent to cause damage.

This is nothing like the situation in *Fidlar Technologies v. LPS Real Estate Data Solutions, Inc.*, 810 F.3d 1075, 1084 (7th Cir. 2016), which Hutchins cites for support. Indeed, in distinguishing the program at issue in that case, the court noted that term "causes damage" under 18 U.S.C. § 1030(a)(5)(C) "encompasses clearly destructive behavior such as using a virus or worm or deleting data . . . [as well as] less obviously invasive conduct, such as flooding an email account." 810 F.3d at

1084. Notably, *Fidlar Technologies* did not speak in any respect to federal *criminal* pleading standards, and neither does any other case cited by Hutchins. *See, e.g., Int'l Airport Ctrs. LLC v. Citrin*, 440 F.3d 418 (7th Cir. 2006) and *Landmark Credit Union v. Doberstein*, 745 F. Supp. 2d 990, 993-94 (E.D. Wis. 2010); *Untied States v. Mitra*, 405 F.3d 492, 493 (7th Cir. 2006).

Because the indictment in this case complies with Rule 7(c)(1), Hutchins's motion to dismiss Counts One and Seven for failure to state an offense should be denied.

C. Counts One through Six state an offense.

Next Hutchins argues Counts One through Six should be dismissed for failure to state an offense because neither Kronos nor UPAS Kit is an "electronic, mechanical, or other device" as defined by § 2010(5). This Court should deny Hutchins's motion because each of these counts: (1) states the elements of the crimes charged, (2) adequately informs the defendant of the nature of the charges brought against him, and (3) enables the defendant to assert the judgment as a bar to future prosecutions for the same offense. *See Vaughn*, 722 F.3d at 925. Even if the Court considered the merits of Hutchins's argument, his motion to dismiss should be rejected, because several courts have held that software known as "spyware" or that has keylogger functionality falls under the Wiretap Act. *See Lius v. Zang*, Nos. 1:11–CV–884, 1:12–CV–629, 2013 U.S. Dist. LEXIS 29288, *6 (S.D. Ohio, March 5, 2013) (collecting cases), *recommendation adopted*, *overruled on other grounds*, *Luis v. Zang*, 833 F.3d 619 (6th Cir. 2016).

In *Lius*, the magistrate judge considered a civil action against the makers of "WebWatcher" software under 18 U.S.C. § 2520. 2013 U.S. Dist. LEXIS at *27. Section 2520 creates a private right of action for anyone whose communication were intercepted, disclosed, or used in violation of the Wiretap Act against the person or entity that engaged in that violation. *See* 18 U.S.C. § 2520(a). The plaintiff in *Lius* alleged the maker of WebWatcher software violated the Wiretap Act because the software had a keylogger function that captured and transmitted data from a computer. *Lius*, 2013 U.S. Dist. LEXIS at *6-9. First, the court in *Lius* held that the WebWatcher software does "intercept" communications under the Wiretap Act. *Id.* at *24-25. The court then went on to assess a software maker's liability under § 2520. The court in *Lius* determined that software manufacturers are excluded from liability under § 2520 because that statute *only* applied to those that "intercepted, disclosed or intentionally used" the intercepted communications. *Id.* at 27-28; *see* 18 U.S.C. § 2520(a).[1]

But unlike the civil case against the defendant in *Lius* brought under § 2520, the government's case against Hutchins is not limited by three activities described in § 2520 (interception, disclosure and use). As alleged in the indictment, Hutchins is charged with selling, sending, and advertising a device to intercept communications, and intercepting and endeavoring to intercept communications. The scope of those activities is broader than those of § 2520, which often exclude

[1] On appeal, the Sixth Circuit found Luis had alleged facts sufficient to show the manufacturer of WebWatcher had intercepted communications. *Luis v. Zang*, 833 F.3d 619, 626-27 (6th Cir. 2016).

software manufacturers from civil liability under that section. And the court in *Lius* is not the only court to find spyware or keylogging software is a device under the Wiretap Act. *See United States v. Barrington*, 648 F.3d 1178, 1201 (11th Cir. 2012) (requiring keylogger software to capture data at the time it is transmitted and beyond the computer on which it is installed to constitute a "device"); *Shefts v. Petrakis*, 2012 U.S. Dist. LEXIS 130542, *8-9 (C.D. Ill. Sept. 13, 2012) (holding spyware that contemporaneously transmitted screenshots from a computer violates the Wiretap Act); *Klumb v. Goan*, 884 F. Supp. 2d. 644, 661 (E.D. Tenn., July 19, 2012) (stating that spyware that automatically routes a copy of an email to through the internet to another party is an interception).

Hutchins relies on *Potter v. Havlicek*, 2008 U.S. Dis. LEXIS 12211 (S.D. Ohio 2008) and *United State v. Szymuszkiewicz*, 622 F.3d 701, 707 (7th Cir. 2010) for the proposition that "software is not a device." Doc. #95at 8. Neither case supports his position.

First, *Potter* dealt with a manufacturer's liability under § 2520. *Potter*, 2008 U.S. Dis. LEXIS 12211, at *14-20. As explained above, § 2520 presents limitation on finding manufacturers liable for civil damages under the Wiretap Act because § 2520 liability only extends to those who intercept, disclose or use the intercepted communications. *Id.* A manufacturer typically does not engage in that conduct, as was the situation in *Potter*. *Id.*

The court in *Szymuszkiewicz* did not address this issue in this case and Hutchins misstates the holding from that case. In *Szymuszkiewicz*, the court

addressed the defendant's argument that "the device" used to intercept a communication must differ from the device the intended audience uses to receive the message." 622 F.3d at 707. The court rejected the defendant's "different device" argument, finding the computer on which the malware was installed was sufficient for violating § 2511(1)(a). *Id.* It never held that "software is not a device."

Because malware like Kronos is a device under the Wiretap Act, and liability is not limited to activities described in § 2520, this Court should deny Hutchins's motion to dismiss Counts One through Six.

Additionally, Counts One, Two, Three, and Six allege violations of the Wiretap Act that are not dependent on Hutchins's limited definition of a device (discussed below). Counts Two and Three allege violation of §§ 2512(1)(c)(i) and (c)(ii), in that Hutchins and his co-conspirator disseminated an advertisement of an "electronic, mechanical, or other device" designed to intercept communications and promoted the use of any other such device. Doc. #86 at 7-8. As described in our responses to Hutchins's other motion to dismiss, Hutchins used a YouTube video and advertisements on internet forums to market the malware. The YouTube video showed a functioning version of Kronos's interception capability. Therefore, even if this Court were to accept Hutchins's position that malware alone does not constitute a device, Counts Two and Three would survive a motion to dismiss because the YouTube video showed the malware operating on a computer. Likewise, the internet posts on hacking forums used to market Kronos describe the

capabilities of the malware on a computer. For those additional reasons, Hutchins's motion to dismiss Counts Two and Three should be denied.

Count Six alleges Hutchins and his co-conspirator "endeavored to intercept, and procured any other person to intercept" communications in violation of §§ 2511(1)(a) and (2). Again, even if the malware alone did not qualify as a "device" under section 2510(5), the fact that the malware was transmitted to another individual, knowing and intending that that individual use the malware to incept communications would constitute a violation of the Wiretap Act under section 2511(1)(a).

It is the same result for Count One. One of the objects of the charged conspiracy was to violate section 2511. Doc. #86. And an illegal agreement to violate section 2511 is not dependent on a "device" as contemplated Hutchins. For example, even if Kronos and UPAS Kit were merely components of an interception device, the development and distribution of that malware would constitute overt acts in furtherance of the conspiracy. *See Read*, 658 F.2d at 1240 (stating conspiracy law punishes the unlawful agreement); *Donner*, 497 F.2d at 190 (7th Cir. 1974) (stating the object of the conspiracy does not need to be accomplished).

To support his positon, Hutchins mainly argues that the Court should adopt one of the definitions of "device" from the internet version of the Merriam-Webster Dictionary, and based on that definition, dismiss Counts One through Six of the indictment. Doc. #95 at 7-9. As Hutchins notes, the Wiretap Act does not further define the terms "any device" or "apparatus." *See* 18 U.S.C. § 2510. Using a

definition from Merriam-Webster's dictionary, Hutchins argues "device" means "a piece of equipment or mechanism designed to serve a special purpose or perform a special function." Doc. #95 at 7. And based on that definition, Hutchins concludes that malware is not a device. *Id.* But that same dictionary defines "mechanism" (from Hutchins's definition above) as "a process, technique, or system for achieving a result." Merriam-Webster Dictionary 2018, *available at* https://www.merriam-webster.com/dictionary/mechanism (last visited on July 26, 2018). And the definition for "device" proffered by Hutchins is the fifth alternative definition. Merriam-Webster Dictionary 2018, *available at* https://www.merriam-webster.com/dictionary/device (last visited April 18, 2018). The first is a "something devised or contrived: such as a . . . procedure, [or] technique." *Id.* Additionally, Merriam-Webster defines "apparatus" as "a set of materials or equipment designed for a particular use" or "the functional process by means of which a systemized activity is carried out." Merriam-Webster Dictionary 2018, *available at* https://www.merriam-webster.com/dictionary/apparatus (last visited April 18, 2018).

Other dictionaries, like the New Webster's Dictionary and Thesaurus define "device" as "something designed or adapted for a special purpose." *New Webster's Dictionary* 261 (Bernard S. Cayne, Lexicon Publications, Inc. 1992). It defines "apparatus" as the "equipment (materials, tools, etc.) needed for a certain task." *Id.* at 43. The Random House Dictionary of the English Language defines "device" as "a thing that is made, usually for a particular working purpose . . . ." Random House

Dictionary (Jess Stein, Random House, Inc. 1979). Looking at the preceding collection of definitions of a "device" and "apparatus" and "mechanism," including the definition preferred by Hutchins, the malware at issue in this case would satisfy the statutory definition of "any device or apparatus" as used in the Wiretap Act.

The definition of "electronic, mechanical, or other device" was also drafted broadly in order to accommodate changing technologies. *See United States v. Mitra*, 405 F.3d 492, 495-96 (7th Cir. 2005) (explaining that Congress writes statutes generally to accommodate new developments in technology); *see also Carter v. Welles-Bowen Realty, Inc.*, 553 F.3d 979, 986 (6th Cir. 2009) (finding that use of the term "any" indicates there are no restrictions as to type or part). This is especially true given the technologies at issue in the Wiretap Act. As the court in *Luis* noted, when the Wiretap Act was first enacted in 1968, "it was designed to protect telephone communications, not email, instant messaging . . . or other forms of electronic, internet-based communication that are commonplace today." *Luis*, 2013 U.S. Dist. LEXIS at *13-15. The transmission of electronic data by a computer was not addressed until 1986 when Congress enacted the Electronic Communications Privacy Act (ECPA). *Id.* As the court in *Luis* noted, "despite its nod to the computer age, when the ECPA was enacted in 1986, email communication was still relatively uncommon" and malware was almost unknown outside academic circles.[2] *Id.* And [a]s often happens when existing laws are used in new ways, courts have struggled

[2] *See* PC Mag.com, Malware: A Brief Timeline found at the following URL on April 17, 2018: https://www.pcmag.com/feature/261678/undefined/feature/261678/malware-a-brief-timeline/undefined/feature/261678/malware-a-brief-timeline/undefined/feature/261678/malware-a-brief-timeline/3

to determine whether, under what circumstances, the Wiretap Act applies to modern and ever-evolving norms of electronic communications." *Id.*

Therefore, the Court should resist Hutchins's attempt to limit the scope of sections 2511 and 2512 based on a definition found in one online dictionary; or because "malware" or "spyware" or "software" is not specifically listed in the definition of "electronic, mechanical, or other device." The reference to "any device or apparatus" is written broadly in order to capture changes in technology. *See Mitra*, 405 F.3d at 495-96. As the Court in *Mitra* noted, [l]egislation is an objective text approved in constitutionally prescribed ways; its scope is not limited by the cerebrations of those [who] voted for or signed it into law. Electronics and communications change rapidly, while each legislature's imagination is limited." 405 F.3d at 495.

Because software constitutes "any device or apparatus" under current case law, Hutchins's motion should be denied. Moreover, as shown above, software or malware fits into the "ordinary meaning" of those terms under the Wiretap Act. And because the definition of "electronic, mechanical, or other device" is broadly written, the Court should apply it broadly. *See Mitra*, 405 F.3d 495 (stating it is the "statutes that [Congress] enacted--not the thoughts they did or didn't have--that courts must apply").

D. Counts Two and Three are not multiplicitous

Hutchins argues that Count Two and Three are multiplicitous and therefore, Count Three must be dismissed. Doc. #95 at 9-10. Counts Two and Three are not multiplicitous because Count Three contains an additional element.

In assessing whether an indictment is multiplicative, courts typically ask "whether each count requires proof of a fact which the other does not. *If one element is required to prove the offense in one count which is not required to prove the offense in the second count, there is no multiplicity.*" *United States v. Conley*, 291 F.3d 464, 470 (7th Cir. 2002) (emphasis added) (citing *United States v. Briscoe*, 896 F.2d 1476, 1522 (7th Cir. 1990) (quoting *United States v. Marquardt*, 786 F.2d 771, 778 (7th Cir. 1986)) (internal citations and quotations omitted))

In his motion, Hutchins correctly asserts that Counts Two and Three "are identical *except* for a signal element." Doc. #95 at 10 (emphasis added). In other words, the government has an additional and different factual burden and element to prove under each count. And that is enough to defeat a claim that the counts are multiplicative. *See Id.*

Even if the Court found that Counts Two and Three were multiplicative, such a finding does not mandate the dismissal of Count Three. The proper remedy for multiplicative counts is merger of those counts. *United States v. Bradbury*, 2015 U.S. Dist. LEXIS 76849, *18-9 (Ind. N.D. June 15, 2015) (relying on *United States v. Platter*, 514 F.3d 782, 786-7 (8th Cir. 2008). As the court in *Bradbury* explained, dismissal of one of the counts would cure the multiplicity problem, but deny the

government its ability to prosecute the case using an alternative theory of liability, which is allowed under Federal Rule of Criminal Procedure 7(c)(1).

E. Counts One, Four through Eight and Ten allege the requisite intent.

Hutchins's final argument is that Counts One, Four through Eight, and Ten[3] should be dismissed because the superseding indictment "does not allege the necessary intent and causation to state those offenses." Doc. #95 at 11. Hutchins's argument should be denied because he is challenging the sufficiency of the evidence he expects at trial, which is beyond the scope of Federal Rule of Criminal Procedure 12. It also appears that Hutchins is once again asking the Court to apply civil pleading standards to a criminal case.

For example, Hutchins complains that the superseding indictment lacks a "claim that [Hutchins and Individual A] intended for the buyers to do anything in particular with the [malware]." Doc. #95 at 12. Hutchins claims "[m]erely writing [a banking Trojan] and selling it - when any illegal activity is up to the buyer to perform - is not enough to allege specific intent by Mr. Hutchins." Doc. #95 at 12. Hutchins also argues a buyer-seller defense to the conspiracy charge. Doc. #95 at 12. Hutchins goes on to argue that "allegations in the indictment" fail to show he is "guilty of the conspiracy charge." Doc. #95 at 13.

Of course, as the Court knows, the government does not have to prove guilt beyond a reasonable doubt through the allegations in an indictment. And it is well

[3] Hutchins fails to address any specific count of the superseding indictment. Hutchins's argument appears to mostly reference the overt acts listed in Count One. To the extent Hutchins failed to develop his argument to any of the counts other than Count One, his motion should be denied as to those counts.

established that an indictment is not evidence. *See* Seventh Circuit Patten Criminal Jury Instruction 1.02 (2012). Federal Rule of Criminal Procedure 7(c)(1) requires an indictment to "be a plain, concise, and definite written statement of the essential facts constituting the offense charged." An indictment is sufficient where it (1) states the elements of the crimes charged, (2) adequately informs the defendant of the nature of the charges brought against him, and (3) enables the defendant to assert the judgment as a bar to future prosecutions for the same offense. *See Vaughn*, 722 F.3d at 925. The superseding indictment in this case satisfies those standards. Hutchins complaints

Because the argument Hutchins makes in support of dismissing Counts One, Four through Eight, and Ten (Section 4, Doc. #95 at 11-14) relates to the sufficiency of the evidence rather than a motion to dismiss under Rule 12, his motion should be denied.

Respectfully submitted,

MATTHEW D. KRUEGER
United States Attorney

By: *s/Michael J. Chmelar*
MICHAEL J. CHMELAR
BENJAMIN W. PROCTOR
Assistant United States Attorneys
Michael Chmelar Bar No.: 6277248
Office of the United States Attorney
Eastern District of Wisconsin
517 E. Wisconsin Ave. Suite 530
Milwaukee, Wisconsin 53202
Tel: (414) 297-1700
Email: michael.chmelar@usdoj.gov
Email: benjamin.proctor@usdoj.gov